BitDefender Mail Protection for Enterprises

EVALUATOR'S GUIDE

bitdefender
secure your every bit

Abstract

This guide introduces evaluators and reviewers to key functions of BitDefender Mail Protection for Enterprises. The objectives of this guide are to provide minimal install instructions and a guided tour of the important features and enhancements in this new release.

This is not intended as a comprehensive explanation of all the features of BitDefender Mail Protection for Enterprises, as such features are presented within the “User's Guide” of the product.

1. Introduction

Thank you for taking the time to evaluate BitDefender Mail Protection for Enterprises.

BitDefender Mail Protection for Enterprises is a complete antivirus and antispam email filtering solution, running at the gates of networks: the email servers. Based on the powerful BitDefender antivirus engines and on the new and improved antispam detection filters, BitDefender Mail Protection for Enterprises is aimed at companies wishing to:

- secure the internal network by limiting the malware threats before reaching the users' workstations
- stop the annoying and even dangerous unsolicited emails, known as spam, and phishing attempts and notify the users about each non trustworthy message
- be protected no matter what email server you run
- be sure to have the latest product updates, even before a malware attack reaches your network
- have a nice and intuitive remote administration console
- be assisted and guided by a valuable 24/7 professional technical support team

This guide for evaluation is designed to allow everyone who is evaluating BitDefender Mail Protection for Enterprises to be able to quickly install, perform standard tests and understand the new features the product offers. For detailed information, you are invited to read the “User's Guide” of BitDefender Mail Protection for Enterprises.

2. Installation

These are just some short installation notes, for a complete description of the installation process and system requirements, please see the accompanying documentation.

BitDefender Mail Protection for Enterprises can be installed on any Linux distribution, using a self-extractable archive. The archive is a compressed tar and includes all the necessary pre-install, post-install, pre-remove and post-remove scripts. This package should be installed using the following command.

```
# ./BitDefender-mpe-{os}-{ver}.{pkg}.run
```

This will unpack the BitDefender files (engines, core, etc.), the install and uninstall scripts.

After unpacking the archive, the installer is launched. This is a text based installer, created to run on very different configurations. Its purpose is to install the extracted packages to their locations and to make the first configuration of BitDefender Mail Protection for Enterprises, asking you few questions. To accept the defaults the installer offers (which is recommended), you only have to press the `ENTER` key.

First, the *Installation directory* is asked. The default is `/opt` and we will assume you go for it. The installer will create the directory `/opt/BitDefender`, which will be the top-level directory of BitDefender Mail Protection for Enterprises, containing several sub-directories, such as `bin`, `etc`, `share`, `var`. If the above-mentioned directory does not exist, you are asked whether the installer should create it, assuming the default *yes*. If you do not agree the directory to be created, the installer will stop.

Also, if a previous BitDefender version is detected, the process will terminate after asking you to remove the old version first.

Next, you are asked what integration agents to install. You can choose one or more from this list.

1. CommuniGate Pro
2. Courier
3. Sendmail Milter
4. qmail
5. SMTP Proxy (for Postfix or any other MTA)

Please enter the corresponding numbers, when prompted, separated by empty spaces. For example, to install the integration agents for *Sendmail Milter* and *qmail*, enter `3 4`.

From this moment, the installer has acquired all the necessary information and will begin the install process. Basically, it will install the engines, the binaries and the documentation and will make the post-install configuration.

After BitDefender Mail Protection for Enterprises has been installed, you have to integrate it in your Mail Transfer Agent. This means you have to redirect the email traffic through the BitDefender integration agents, for each message to be scanned. All you have to do is to run the next command, specifying the desired Mail Transfer Agent, for example `qmail`.

```
# bdsafe agent integrate qmail
```

Eventually, enable the agent.

```
# bdsafe agent qmail enable
```

3. Quick tests

Let's run some short tests to see whether BitDefender is working and, most of all, how it is working. We will address separately the major components: the antivirus and the antispam functions.

To make sure BitDefender is working properly, we will test its efficiency using standard testing methods. Basically, you will have send a special email to some account through the email server. You will receive the results (disinfected email, notifications or the email marked as SPAM). Alternately, you can watch the statistics BitDefender will report.

3.1. Antivirus test

For the antivirus test, we will simulate an infected email reaching the email server. It is a simulation since no real virus is to be used, but a standard test file, known as EICAR. Let's introduce it.

EICAR

You can verify that the BitDefender Antivirus component works properly with the help of a special test file, known as *EICAR Standard Anti-virus Test* file. EICAR stands for the *European Institute of Computer Anti-virus Research*. This is a dummy file, detected by the various antivirus products.

There is no reason to worry, because this file is not a real virus. All that `EICAR.COM` does when executed is to display the text `EICAR-STANDARD-ANTIVIRUS-TEST-FILE` and exit.

The reason we do not include the file within the package is that we want to avoid generating any false alarms for those who use BitDefender or any other virus scanner. However, the file can be created using any text editor, provided the file is saved in standard MS-DOS ASCII format and is 68 bytes long. It might also be 70 bytes if the editor puts a `CR/LF` at the end. The file must contain the following single line:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Copy this line and save the file with any name and .COM extension, for example EICAR.COM. You can keep the EICAR.COM in a safe place and test periodically the server protection.

EICAR online resources

You can visit the EICAR website at http://eicar.com/, read the documentation and download the file from one of the locations on the web page http://eicar.com/anti_virus_test_file.htm.

Infected email attachment

For testing the email protection efficiency, create an email with your favorite email agent, attach the file EICAR.COM and send it to yourself through your email server. You will shortly receive the email disinfected, the notification emails as postmaster and, if configured, the emails addressed to sender and receiver stating about the virus found.

If you have no Linux to work with, feel free to use any other Operating System and email agent. Just follow the above steps: compose a new email, attach the EICAR file and send it. It is preferable to send it to yourself, as you will see the result immediately.

Sending the email to another account

The $USER parameter is used to send the email to your current account on local machine. If you wish to send the test emails to another recipient or to some remote email server, replace it with a real email address, but take care the emails will be classified as infected and/or spam.

Using the **mail** program, available on many Linux distributions, sending the email can be done in the following way. You can safely replace **mail** with **mutt** or **nail**, if your **mail** does not support attachments.

```
$ echo "EICAR test file." | mail -s EICAR -a EICAR.COM $USER
```

Alternately, if your version of **mail** program does not support attachments, you can use the next command, where the email body is just the content of EICAR.COM file (since it is an ASCII file). BitDefender, scanning the entire email, will find it infected, will disinfect it and will notify the postmaster and, eventually, the sender and the receiver.

```
$ mail -s EICAR $USER < EICAR.COM
```

Here is what you will see. First, you will receive the email disinfected, containing a note saying what virus has been found and what happened to it. If you look at the log file, there will be a line about the event: arriving of the email and disinfection. And finally, there are the notification emails sent to the server administrator and to the sender, if the notifications have been enabled.

Infected attached archive

For testing the efficiency of the BitDefender MIME Packer component, create an archive containing the `EICAR.COM` file, then attach it to an email sent to yourself through the email server to test. For example, **gzip** the `EICAR.COM` file and attach the resulting archive.

```
$ gzip --best EICAR.COM
$ echo "EICAR test archive." | mail -s EICAR -a EICAR.COM.gz $USER
```

You will shortly receive the email disinfected, the notification emails as postmaster and, if configured, the emails addressed to sender and receiver stating about the virus found.

3.2. Antispam test

GTUBE

You can verify that BitDefender Antispam component works properly with the help of a special test, known as *GTUBE*. GTUBE stands for the *Generic Test for Unsolicited Bulk Email*. GTUBE provides a test by which you can verify that BitDefender filter is installed correctly and is detecting incoming spam.

GTUBE online resources

You can visit the GTUBE website at http://gtube.net/, read the documentation and download the sample RFC-822 format email from the locations on the web page.

The test consists in entering the following 68-byte string, as one line, in the body of the email:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

When scanning the email, BitDefender must tag it as spam.

Using the **mail** program, you can test BitDefender with the next command. You have to create a file, named `GTUBE`, containing on one line the above string. Then, run the following command.

```
$ mail -s GTUBE $USER < GTUBE
```

You will shortly receive the email marked as SPAM. The `Subject` will have the following form:

```
Subject:  [spam] GTUBE
```

If you take a look at the email headers, you will notice this one:

```
X-BitDefender-Spam:  Yes (100)
```

Now it is easy to create filtering rules based on the subject or, better, on the `X-BitDefender-Spam` header.

RBL quick configuration

The RBL filter servers to filter spam based on mail server's reputation as spam sender. To configure it, you can use the **bdsafe** command. More information can be obtained from the User's Guide or from the **bdsafe** manual page.

Basically, you have to set a DNS server and one or more RBL servers, along with their trust level.

To set the DNS server, use the following command. Use the IP address of the server.

```
# bdsafe configure rbl dnsserver 1.2.3.4
```

To add a new RBL server to the list, use the next command, specifying the hostname and the trust level.

```
# bdsafe configure rbl servers add sbl-xbl.spamhaus.org,90
```

Finally, do not forget to enable the RBL filter.

```
# bdsafe group configure userblfilter Y
```

4. New and improved features

We have just presented the basic functionality of BitDefender Mail Protection for Enterprises. But there is more.

4.1. Group management

The BitDefender Group Management component is used to manage users and settings as groups in a very flexible way. It can be easily integrated with any application requiring this feature.

Basically, there are groups and user. The users are defined according to their email address or login name, as they are seen by the server internally. Several users define a group. The nice part is just following: you can specify various settings for each group, such as antivirus actions, templates to be used for notification and so on.

There are two special groups: `All` and `Default`. The group `All` concentrates the settings for all users, as expected, and the `Default` group specifies the implied settings, if they are not defined in a certain group.

Let's play with the groups. We shall create a new one, add some users inside and apply some settings.

First, a new group has to be created. Let's name it `MyGroup` and add two users identified by their email addresses: `user1@example.com` and `user2@example.com`. Open a terminal and run the following, as root.

```
# bdsafe group insert MyGroup sender user1@example.com user2@example.com
```

We should clarify some things, before proceeding to the next step. The **bdsafe** command is the main BitDefender configuration tool. It should be wise to have a look at the bdsafe(8) manual page, to get an idea about its options and usage.

Second, the `sender` option will identify the users only as email senders. If you need to identify them as receivers, change it to `recipients`.

At this moment, we can list the groups and the users to check the previous command worked. Here is the command you should run.

```
# bdsafe group list MyGroup
```

Now, we have a group and some users inside the group. Let's change the antivirus actions to `disinfect;quarantine`. We have to use the same **bdsafe**. Please do not forget to study the manual page for details.

```
# bdsafe group configure MyGroup antivirus actions disinfect;quarantine
```

Let's use the `Default` group, too: by default, the email footers should not be appended. Here is the command.

```
# bdsafe group configure Default addfooters false
```

4.2. SNMP

The SNMP support of BitDefender Mail Protection for Enterprises consists of two implementations: a SNMP plugin and a Logger plugin.

The Net-SNMP plugin, is a module of the **snmpd** daemon (developed for the `net-snmp` package). It is loaded by the daemon and communicates with BitDefender Registry to gain read and write access to BitDefender settings.

The second implementation, the Logger plugin, is just another module beside file logger, real-time virus and spam report module or mail notification module. It receives the same BitDefender events information as the others Logger Plugins and sends them to some remote host running the SNMP trap server, which, in turn, will process them (send to syslog, etc.).

The NET-SNMP plugin

As stated before, this is a plugin loaded by `net-snmp`, used to interrogate and, eventually, modify the BitDefender settings.

Let's start by verifying that you have the plugin. It should be located at `/opt/BitDefender/var/lib/libbduxsnmp.so`. And you will need one more thing: the mib file `BITDEFENDER-MIB.txt` that you should copy to the above mentioned `mibs` directory.

Please see the accompanying documentation for installation instructions.

Walking through the MIBs

Make sure **snmpd** is up and run the next command. You will get a list of the SNMP keys you can interact to.

```
# snmpwalk -v 3 -m ALL -u bitdefender -l authPriv -a MD5  \
           -A <authpass> -x DES -X <privpass> localhost softwin
```

BitDefender plugin works also with versions 1 and 2c, but you need the community string (which is `public` by default). For example, the following line uses the version 1.

```
# snmpwalk -v 1 -m ALL -c public localhost softwin
```

There are some graphical tools to play with. For example, the `net-snmp` package contains **tkmib**, a Tk-based SNMP client tool. You can find our module at `.iso.org.dod.internet.private.enterprises.softwin`, after loading the MIB, of course.

With this plugin, you will be able to do the following.

- Monitor the BitDefender Daemons.
- Force an update via the `cupdate` key.
- Consult the global statistics.

- Consult the update related keys: last update, last check, update status and set the interval between to successive checks.
- Consult the number of signatures of the antivirus engine.
- Consult the license information: the license type, the number of users, the number of domains (reported to the total number of users and domains supported by the license).

Get and set values

You can also get and set individual values in the tree, using this plugin. But you need to specify the read-only and read-write communities in `/etc/snmp/snmpd.conf` file. Add the following two lines.

```
rocommunity public
rwcommunity private
```

Now, to get a value use this line. It will return the time between two consecutive updates.

```
# snmpget -v 1 -m ALL -c public localhost checksecs.0
```

To set a value, for example to trigger an update, run this command.

```
# snmpset -v 1 -m ALL -c private localhost cupdate.0 s "y"
```

The BitDefender Logger plugin

The BitDefender Logger receives messages from various BitDefender components and presents them to the user in various formats. It can log the messages to a file, forward them by email to a designated address or, using this plugin, it can send them to a SNMP server.

Configuration

The messages sent to the SNMP server are received by the **snmptrapd** daemon. We need to configure it. But first, please make sure the SNMP services are not running.

We need an username for SNMP version 3 protocol. If you like to use the version 1 or 2c, you do not need the user and you can skip over the following paragraphs.

Let's use the same `bitdefender` username as above. Make sure there is this line in the `/etc/snmp/snmpd.conf` file.

```
rwuser bitdefender
```

Thus we specify this user will have read and write access, but it is not defined yet. Add this line at the end of the `/var/net-snmp/snmptrapd.conf` file and remember the passwords should be longer than 8 characters. If the file does not exist, just create it.

```
createUser -e 0xBD224466 bitdefender MD5 <authpass> DES <privpass>
```

If you plan to use the `INFORM` alerts, without need for the EngineID, you will have to add an user without specifying the EngineID. The user defined in the line above will not work, so add a new one.

```
createUser bitdefender_inform MD5 <authpass> DES <privpass>
```

Let's stop a while and explain this line. You are free to change anything in it with the only condition to reflect the changes in the BitDefender configuration.

`-e 0xBD224466`
: This is the EngineID. It is mandatory for alerts of `TRAP` type and optional for `INFORM` type. The alert type should be specified in `/BDUX/LoggerDaemon/Plugins/SNMP/AlertType` registry key.

  The EngineID must be specified also in the BitDefender registry at `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityEngineID` key. If not used (it is optional when the alerts type is `INFORM`), the `SecurityEngineID` key must be empty.

`bitdefender`
: This is the user to create for authenticated SNMP v3. The same name should be declared in the `/etc/snmp/snmpd.conf` (please read above) and in `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityName` registry key.

`MD5`
: The authentication protocol (`MD5` or `SHA1`) used for authenticated SNMP v3. The same value must be found in `/BDUX/LoggerDaemon/Plugins/SNMP/AuthProto` registry key.

<authpass>
: Set the authentication pass phrase used for authenticated SNMP v3 messages. The same value must be found in `/BDUX/LoggerDaemon/Plugins/SNMP/AuthProtoPass` registry key.

`DES`
: Set the privacy protocol (`DES` or `AES`) used for encrypted SNMP v3 messages. The same value must be found in `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityPrivProto` registry key.

<privpass>
Set the privacy pass phrase used for encrypted SNMP v3 messages. The same value must be found in `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityPrivProtoPass` registry key.

This line will be replaced with another one, with encrypted passwords, when **snmptrapd** daemon is started.

One more thing: you do not need to use all the parameters specified above for SNMP v3. You can use the authentication without encryption (the `SecurityLevel` key is `authNoPriv`) or no authentication and no encryption (the `SecurityLevel` key is `noAuthNoPriv`). You have to modify the `createUser` line accordingly.

This would be the user. Now, let's get back to the `/etc/snmp/snmpd.conf` file and added some more lines. You might find them already in your file, but commented out. Uncomment them and set the correct values.

```
# trapsink: A SNMPv1 trap receiver
trapsink  localhost

# trap2sink: A SNMPv2c trap receiver
trap2sink  localhost

# informsink: A SNMPv2c inform (acknowledged trap) receiver
informsink  localhost public

# trapcommunity: Default trap sink community to use
trapcommunity  public

# authtrapenable: Should we send traps when authentication
#                 failures occur
authtrapenable  1
```

I think this is the moment to start the **snmpd** and **snmptrapd** daemons. If you get an error, please review the configuration.

Usage

Now you can test the SNMP server. Here are some commands you may start with. The first one will send `TRAP` alert that should be logged on syslog. Please note we use the EngineID.

```
# snmptrap -e 0xBD224466 -v 3 -m ALL -u bitdefender -l authPriv    \
           -a MD5 -A <authpass> -x DES -X <privpass> localhost 42  \
           coldStart.0
```

Another command sends an `INFORM` alert. In this case, there is no need to specify the EngineID and the user you have created must not have the EngineID. In our examples,

we have created the `bitdefender_inform` user for this purpose. The alert will be logged on syslog too.

```
# snmpinform -v 3 -m ALL -u bitdefender_inform -l authPriv -a MD5  \
             -A <authpass> -x DES -X <privpass> localhost 42       \
             coldStart.0
```

If you do not want to use the SNMP version 3 protocol, you can use the other two supported: 1 and 2c. In this case you do not need the username, all you have to know is the community string. This is `public` by default. For example, for version 2c, use this command.

```
# snmptrap -c public -v 2c -m ALL localhost 42 coldStart.0
```

If everything is all right and BitDefender is properly configured (that means the registry keys fit the SNMP server configuration), all you have to do is to enable the plugin (if not already enabled) and try it by sending emails through the MTA. You will shortly see the report on the syslog of the machine running the SNMP server.

4.3. Update

The BitDefender update process is realized by Live! Update, a daemon which connects periodically to the BitDefender update server and checks whether new virus definitions, antispam updates and product upgrades are available. In case there are any, the daemon will download only the changed files, executing an incremental update and conserving the bandwidth.

Automatic update

BitDefender Mail Protection for Enterprises is configured to update automatically each 8 hours, through **bdlived** module. In case of a necessary update, before the specified interval expires, the daemon can be signaled to execute the update routine, manually. To trigger the on-demand check, one can issue following command, using **bdsafe(8)**.

```
# bdsafe update
```

The command will output nothing, but, if you check the log file, you will see a line stating that the update process has been triggered.

You can check the update module configuration at any time. Just use the bdsafe again.

```
# bdsafe configure update
```

Time interval modification

To modify the time interval, let's say to 2 hours, you will have to run the command bellow.

```
# bdsafe configure update checkinterval 7200
```

Live! Update proxy configuration

If a proxy server is to be used to connect to the Internet please run the following command providing the correct settings, the proxy address and port.

```
# bdsafeconfigure update proxysettings address:port
```

By default, the proxy is disabled. To enable it, use this command.

```
# bdsafeconfigure update useproxy Y
```

Update Pushing

Update Pushing is an ordered update launched by the BitDefender servers in imminent situations, when a prompt update can save the server from allowing the infected emails to pass.

The trigger is an email, sent to the address you have specified during the installation. BitDefender, while filtering the emails, will recognize it and will initiate the update process. Then, the email can be dropped or delivered, as you wish.

Patches

Since the Live! Update module can update automatically only the virus definitions and some of the core libraries used by BitDefender, there is a small tool that can be used to update the whole BitDefender installation.

BitDefender Swiss Army kniFE, **bdsafe(8)**, is a multipurpose tool used for keeping BitDefender up to date by applying various patches that might appear after the product was released. It can be run directly by the system administrator to list, search, install or uninstall patches or it can be installed as a cron job to automatically install the patches as soon as they are released.

Patches are released to correct any bugs found or to add new features and they are grouped in the following categories: **CRITICAL**, **SECURITY**, **NORMAL**.

- Patches are labeled **CRITICAL** when they affect the normal behavior of the product. For example, if a new kernel is released, preventing the **bdcored** module to accomplish its job, then a **CRITICAL** patch will be released, correcting this issue.

- A patch is labeled **SECURITY** when it has the role to correct any security related issue. For example, if there is a bug which might permit an attacker to gain access to emails scanned by BitDefender, then a **SECURITY** patch will be released to fix this issue. Opposed to **CRITICAL** patches, which affect the BitDefender's normal behavior, **SECURITY** patches can fix the bugs that will not occur in friendly environment, if such one exists, usually.
- Patches labeled **NORMAL** are usually released to fix minor (cosmetic) bugs or to add some new features. For example, if BitDefender incorrectly formats an email header, a **NORMAL** patch will be released to fix this minor issue.